



# Tenable Vulnerability Management and Thycotic Integration Guide

---

Last Revised: July 11, 2023



# Table of Contents

<b>Introduction</b> .....	<b>3</b>
<b>Integration Requirements</b> .....	<b>4</b>
<b>Integrate with Thycotic Secret Server</b> .....	<b>5</b>
Configure Windows Credentials .....	6
Configure Linux Credentials .....	11
<b>Troubleshooting</b> .....	<b>16</b>



---

## Introduction

---

This document describes how to deploy Tenable Vulnerability Management for integration with Thycotic Secret Server. Please email any comments and suggestions to Tenable Support.

Security administrators know that conducting network vulnerability assessments means getting access to and navigating an ever-changing sea of usernames, passwords, and privileges. By integrating Thycotic Secret Server with Tenable Vulnerability Management, administrators now have even more choice and flexibility for reducing the credentials headache.

The Tenable® integration with Thycotic Secret Server delivers a comprehensive authenticated scanning solution that provides security teams better vulnerability insight in order to further protect privileged accounts. This integration supports the storage of privileged credentials in Thycotic Secret Server and their automatic retrieval at scan time by Tenable. This ensures that sensitive passwords are safely stored, controlled, auditable and easily changed without manual intervention.

By integrating Tenable Vulnerability Management with Thycotic Secret Server, you can:

- Store credentials in Thycotic Secret Server instead of managing and updating the credentials directly within a Tenable solution.
- Reduce the time and effort needed to document credential storage within the organizational environment.
- Automatically enforce security policies within specific departments or for specific business unit requirements, simplifying your compliance process.
- Reduce the risk of unsecured privileged accounts and credentials across the enterprise.



---

## Integration Requirements

---

You must meet the following minimum version requirements to integrate Tenable Vulnerability Management with Thycotic Secret Server:

- Thycotic Secret Server version 8.9 or later
- Tenable Vulnerability Management, Tenable's cloud platform for vulnerability management

**Note:** The integration requires enabling the Thycotic Secret Server web services API, which is available in Secret Server Professional and the hosted version of Secret Server.



---

## Integrate with Thycotic Secret Server

---

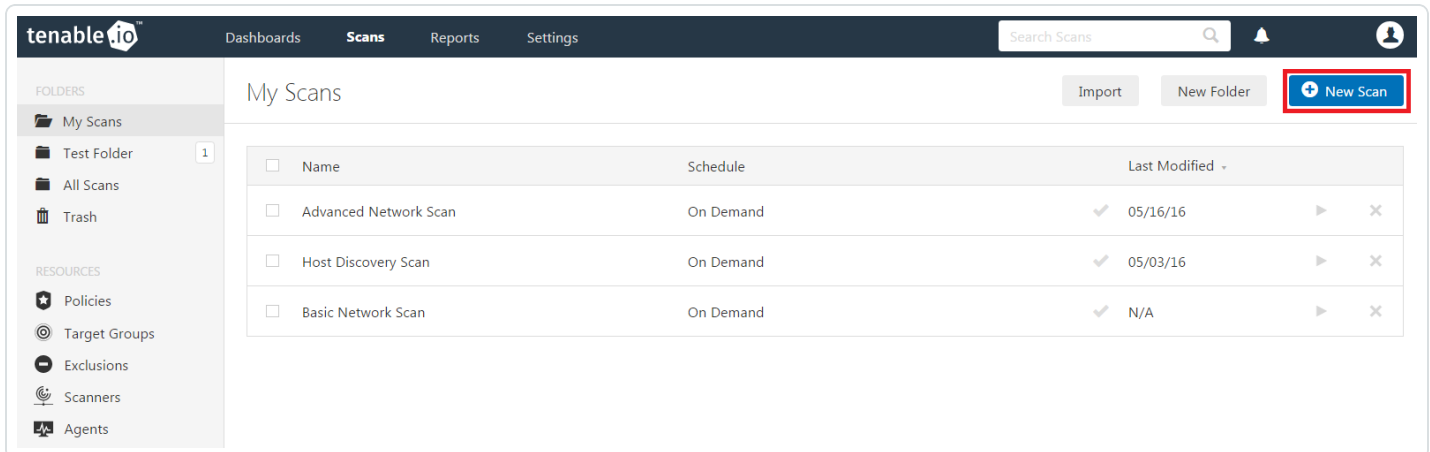
You can configure Tenable Vulnerability Management to perform credentialed network scans of Windows and Linux systems using Thycotic's password management solution. Credentials are configured similarly to other credentialed network scans.

[Configure Windows Credentials](#)

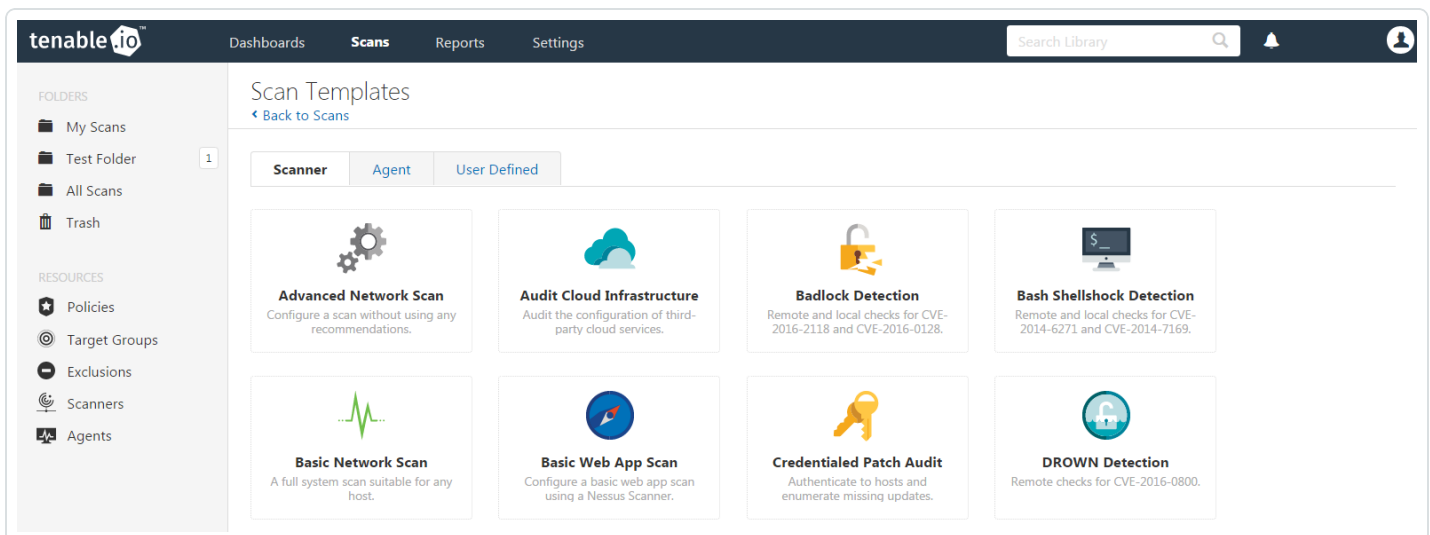
[Configure Linux Credentials](#)

# Configure Windows Credentials

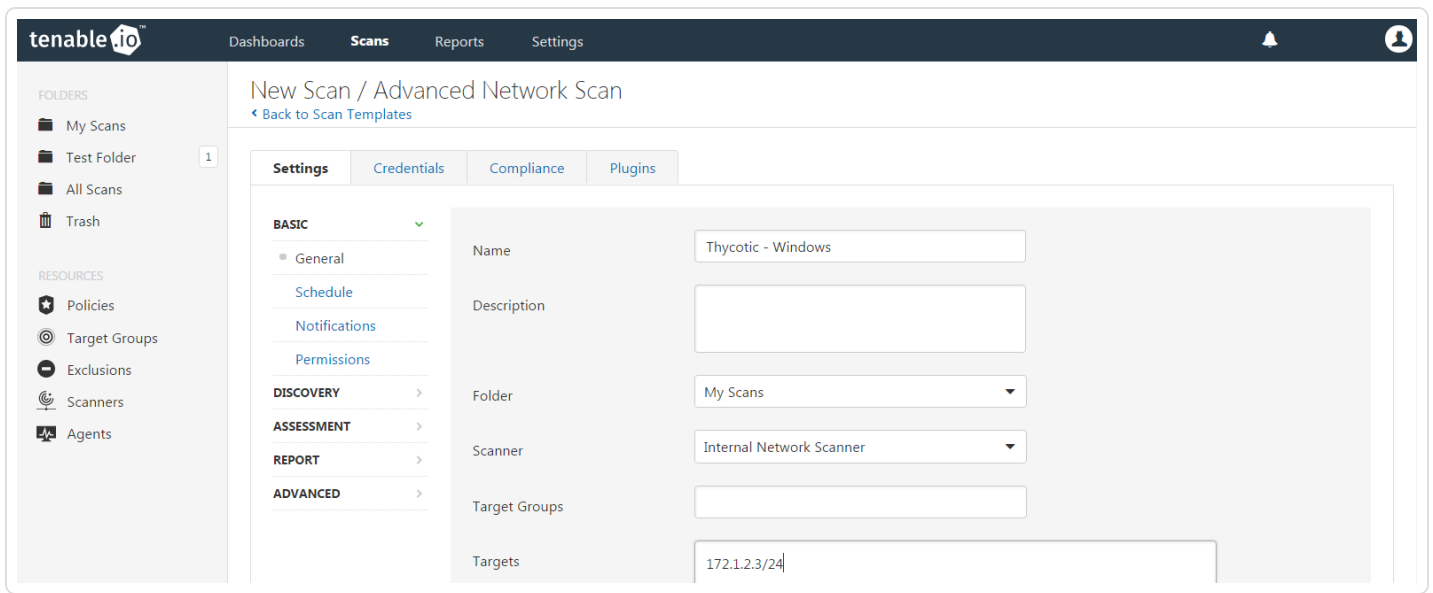
Log in to Tenable Vulnerability Management and click **Scans** and then the **+ New Scan** button to configure Tenable Vulnerability Management for credentialed scans of Windows systems using Thycotic's password management solution.



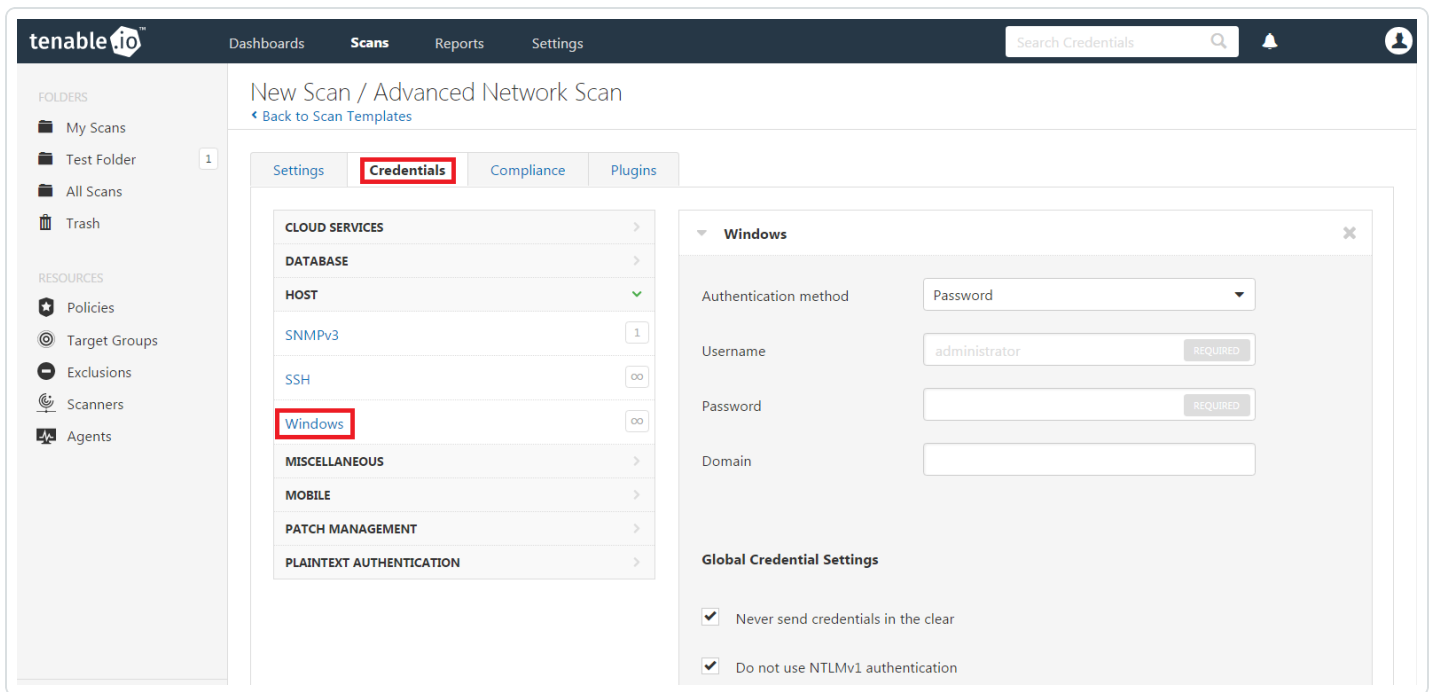
Select a "Scan Template" for the scan type required for your scan. For demonstration purposes, the "Advanced Network Scan" template will be used.



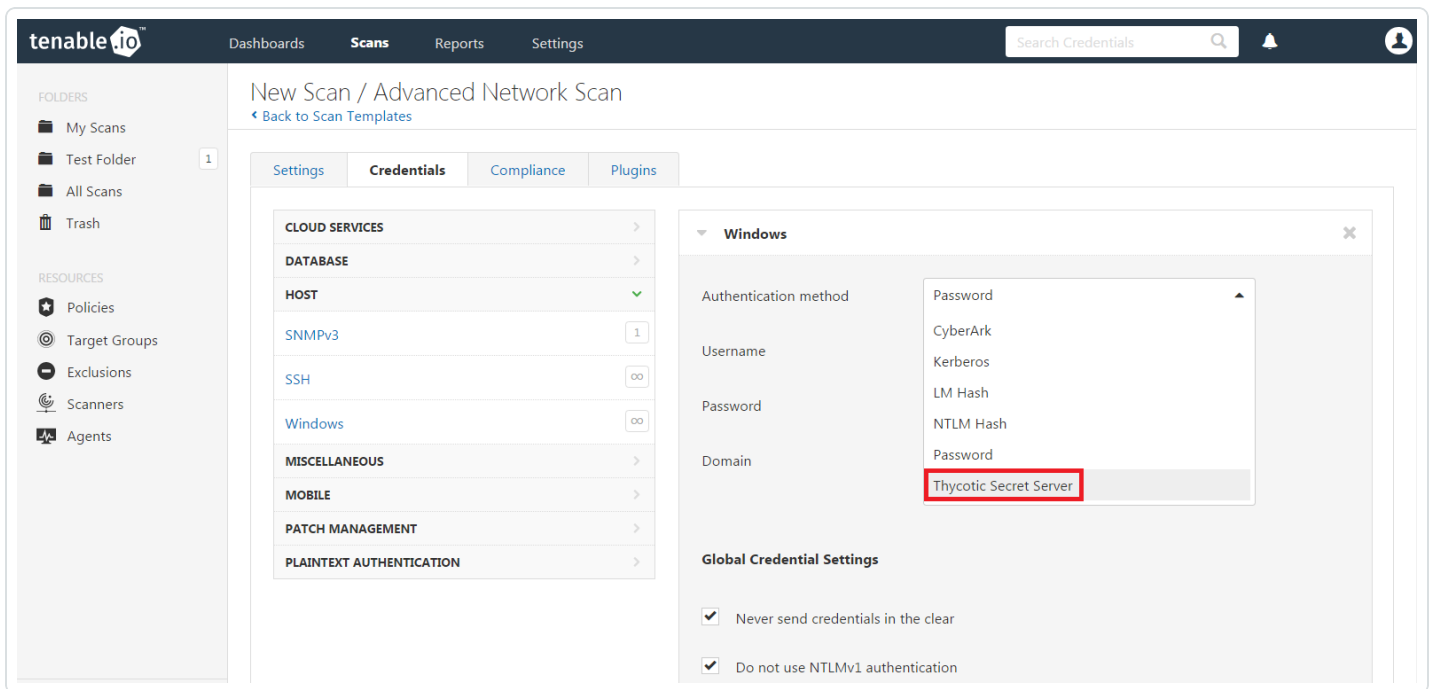
To configure a credentialed scan for Windows systems using Thycotic's password management solution, enter a descriptive **Name** and enter the IP address(es) or hostname(s) of the scan **Targets**.



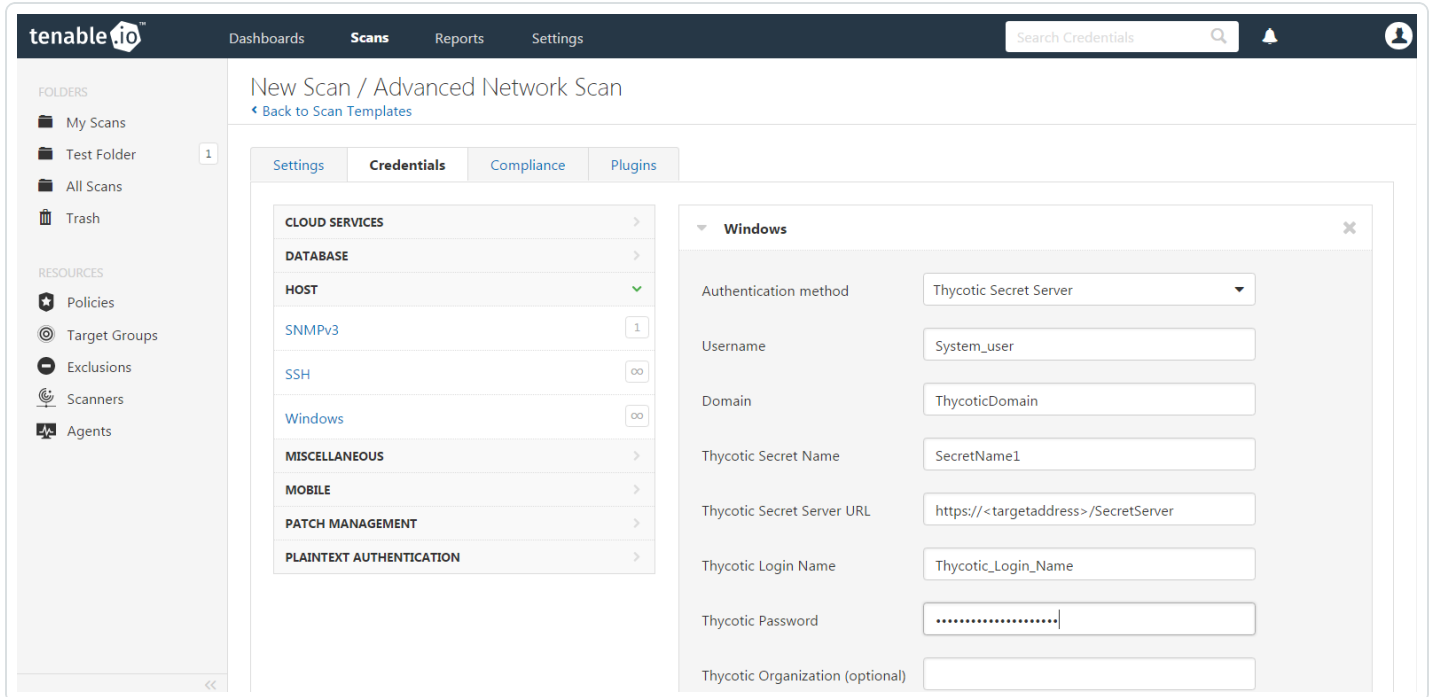
Once the “Name” and “Targets” have been configured, click on **Credentials** and then select **Windows** from the left-hand menu.



Click the **Authentication method** drop-down and select **Thycotic Secret Server**.



Configure each field for Windows authentication. Refer to “Table 1 - Thycotic Windows Credentials” below for a description of each field. Once the Windows credentials have been configured, click **Save** to finalize the changes.



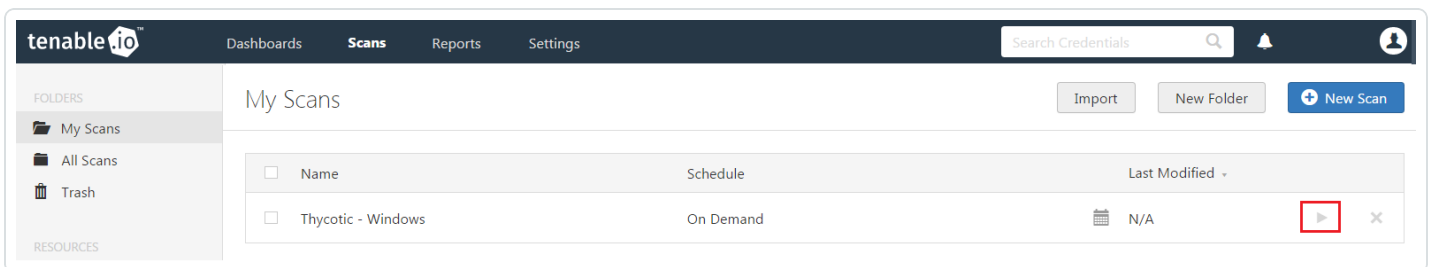
*Table 1 - Thycotic Windows Credentials*





Option	Description
Username	The target system(s) username
Domain	This is an optional field if the above username is part of a domain
Thycotic Secret Name	The value (“Secret Name”) that the secret is stored as on the Thycotic server
Thycotic Secret Server URL	URL of the Thycotic Secret Server, which sets the transfer method, target, and target directory. This information can be found in Admin > Configuration > Application Settings > Secret Server URL on the Thycotic server.
Thycotic Login Name	The username used to authenticate to the Thycotic server
Thycotic Password	The password associated with the Thycotic Login Name
Thycotic Organization (optional)	This is an optional value used in cloud instances of Thycotic to define which organization should be queried
Thycotic Domain (optional)	This is an optional value set if the domain value is set for the Thycotic server
Verify SSL Certificate	Use the Custom_CA setup method to validate SSL server certificates

To verify the integration is working, click the **Launch button** to initiate an on-demand scan.



Once the scan has completed, select the completed scan and look for “Plugin ID 10394” (shown below), which validates that authentication was successful. If the authentication is not successful, refer to the [Troubleshooting](#) section of this document.



tenable.io | Dashboards | Scans | Reports | Settings | Search Credentials | [User Profile]

192.168.1.106 | [Configure] | [Export]

[Back to Windows 10](#)

**Vulnerabilities** 1

Sev	Name	Family	Count
●	Microsoft Windows SMB Log In Possible	Windows	1

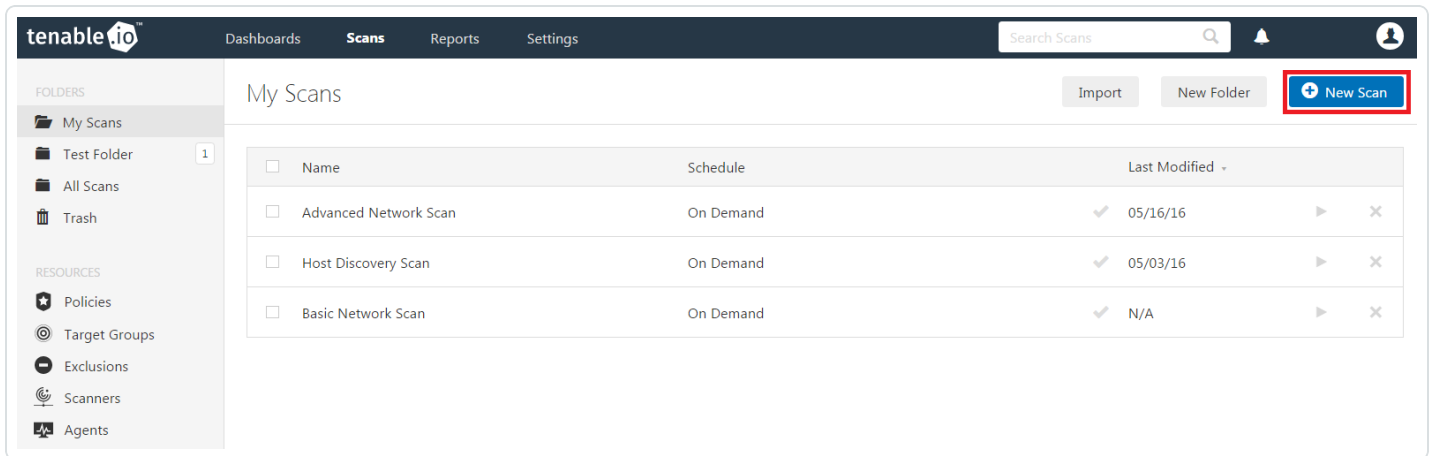
**Host Details**

IP: 192.168.1.106  
MAC: 0c:8b:fd:52:05:1c  
OS: Microsoft Windows 10 Home  
Start: January 3 at 10:44 AM  
End: January 3 at 10:50 AM  
Elapsed: 6 minutes

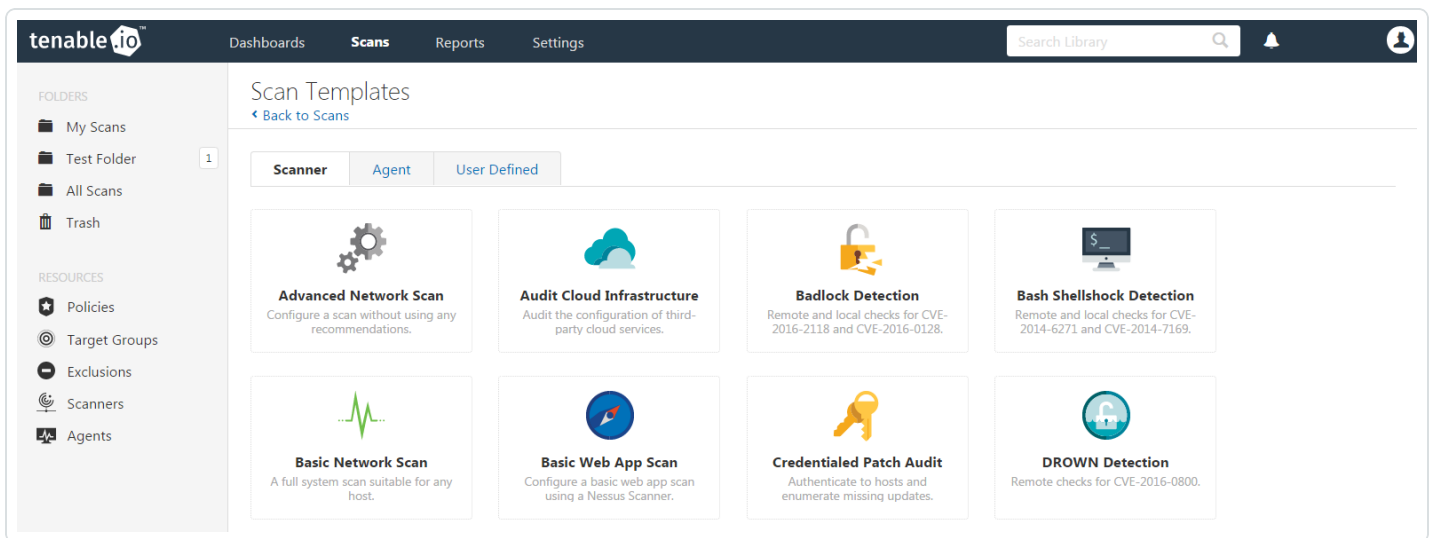
# Configure Linux Credentials

Configuring Linux credentialed scans follows the same basic steps as Windows credentialed scans with only a few minor differences.

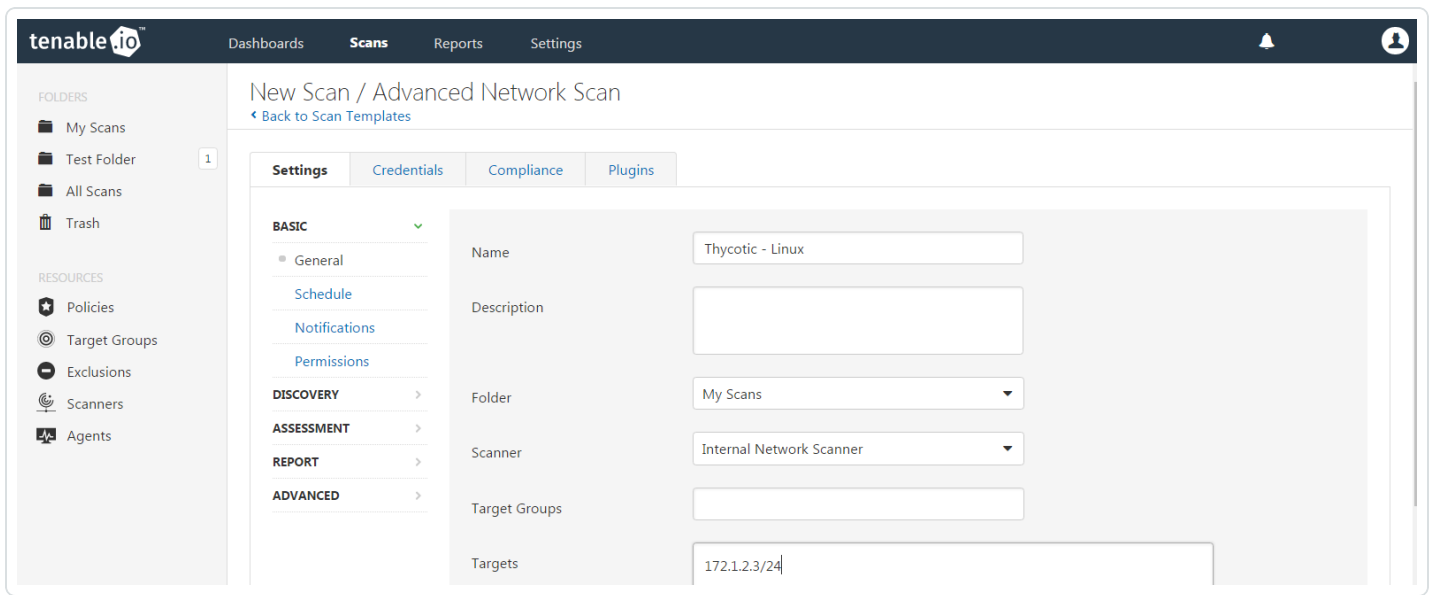
Log in to Tenable Vulnerability Management and click **Scans** and then the **+ New Scan** button to begin the Linux credentialed scan configuration.



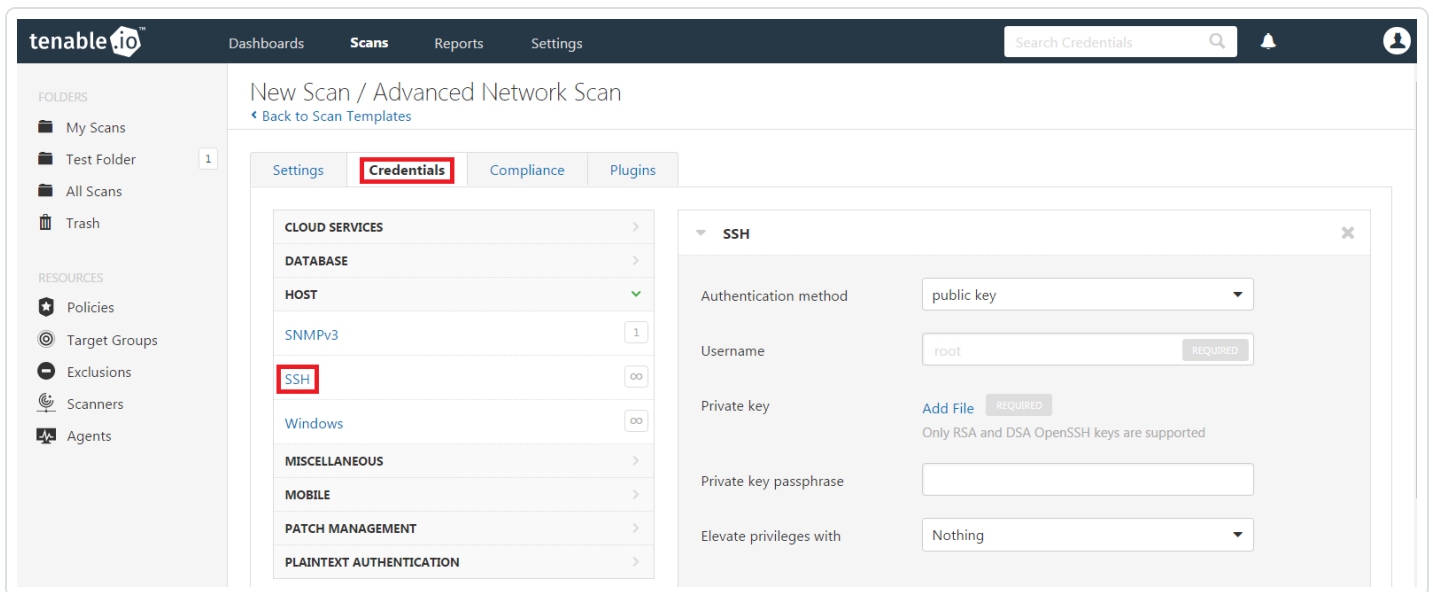
Select a “Scan Template” for the scan type required for your scan. For demonstration purposes, the “Advanced Scan” template will be used.



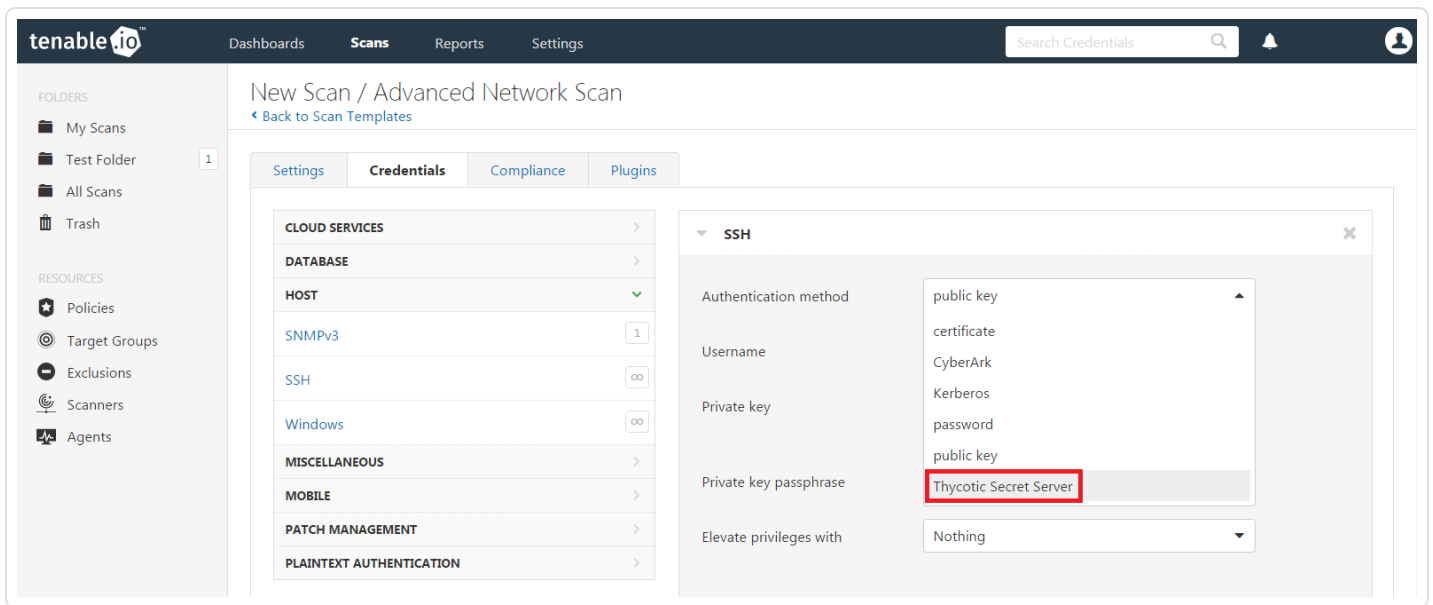
To configure a credentialed scan for Linux systems using Thycotic’s password management solution, enter a descriptive **Name** and enter the IP address(es) or hostname(s) of the scan **Targets**.



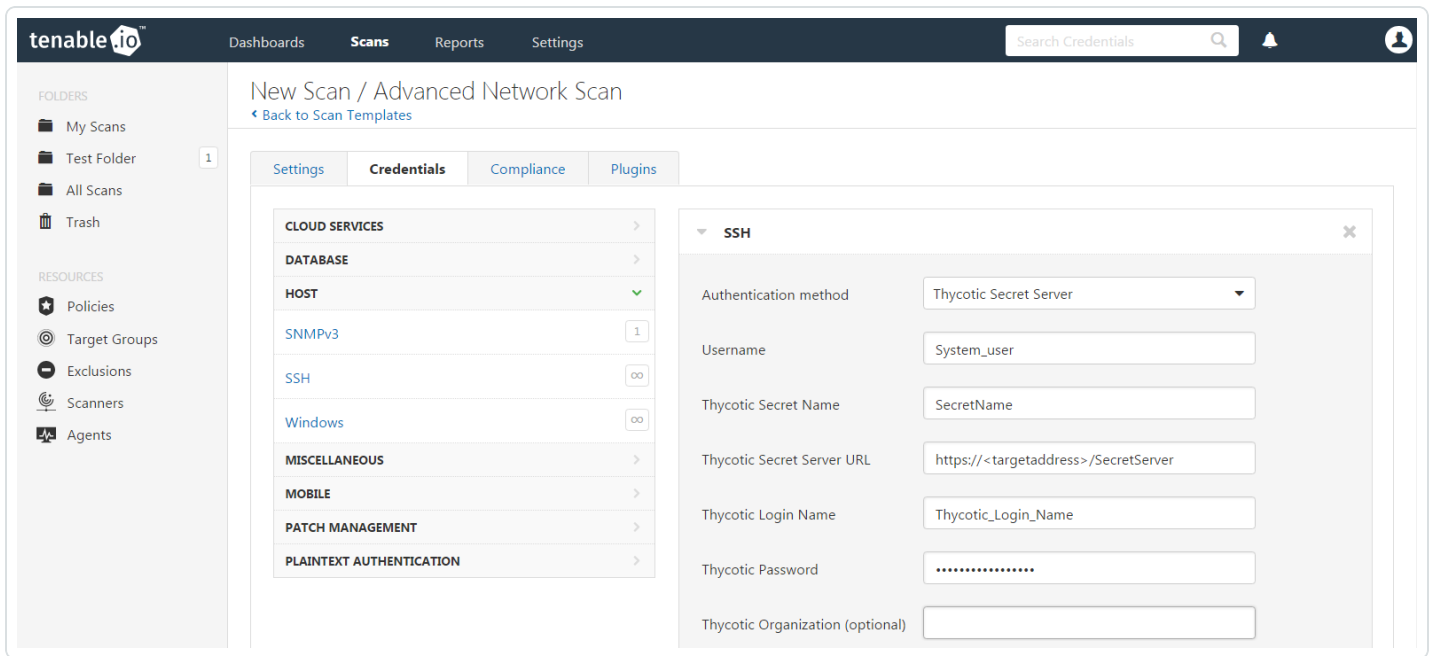
Once the “Name” and “Targets” have been configured, click on **Credentials** and then select **SSH** from the left-hand menu.



In the **Authentication method** drop-down box, select **Thycotic Secret Server**.



Configure each field for SSH authentication. Refer to “Table 2 - Thycotic SSH Credentials” below for a description of each field. Once the SSH credentials have been configured, click **Save** to finalize the changes.



*Table 2 - Thycotic SSH Credentials*

Option	Description
Username	The username that is used to authenticate via ssh to the system.



Thycotic Secret Name	This is the value that the secret is stored as on the Thycotic server. It is referred to as the “Secret Name” on the Thycotic server.
Thycotic Secret Server URL	This is used to set the transfer method, target , and target directory for the scanner. The value can be found in <b>Admin &gt; Configuration &gt; Application Settings &gt; Secret Server URL</b> on the Thycotic server. For example consider the following address <code>https://pw.mydomain.com/SecretServer/</code> . We will parse this to know that <code>https</code> defines it is a ssl connection, <code>pw.mydomain.com</code> is the target address, <code>/SecretServer/</code> is the root directory.
Thycotic Login Name	The username used to authenticate to the Thycotic server.
Thycotic Password	The password associated with the <b>Thycotic Login Name</b> .
Thycotic Organization (optional)	This value is used in cloud instances of Thycotic to define which organization your query should hit.
Thycotic Domain (optional)	This is an optional value set if the domain value is set for the Thycotic server.
Use Private Key	Use key based authentication for SSH connections instead of a password.
Verify SSL Certificate	Verify if the SSL Certificate on the server is signed by a trusted CA.
Thycotic elevate privileges with	<p>The privilege escalation method you want to use to increase the user's privileges after initial authentication. Multiple options for privilege escalation are supported, including <code>su</code>, <code>su+sudo</code> and <code>sudo</code>. Your selection determines the specific options you must configure.</p> <div style="border: 1px solid blue; padding: 5px;"><p><b>Note:</b> For additional information about all of the supported privilege escalation types and their accompanying fields, see <a href="#">Host</a> in the Tenable Vulnerability Management User Guide.</p></div>

To verify the integration is working, click the **Launch button** to initiate an on-demand scan.

The screenshot shows the Tenable.io interface. At the top, there is a navigation bar with 'tenable.io', 'Dashboards', 'Scans', 'Reports', and 'Settings'. A search bar for 'Search Credentials' and a user profile icon are also present. On the left, a sidebar lists 'FOLDERS' (My Scans, All Scans, Trash) and 'RESOURCES'. The main content area is titled 'My Scans' and contains a table with the following data:

<input type="checkbox"/>	Name	Schedule	Last Modified -	
<input type="checkbox"/>	Thycotic - Linux	On Demand	N/A	

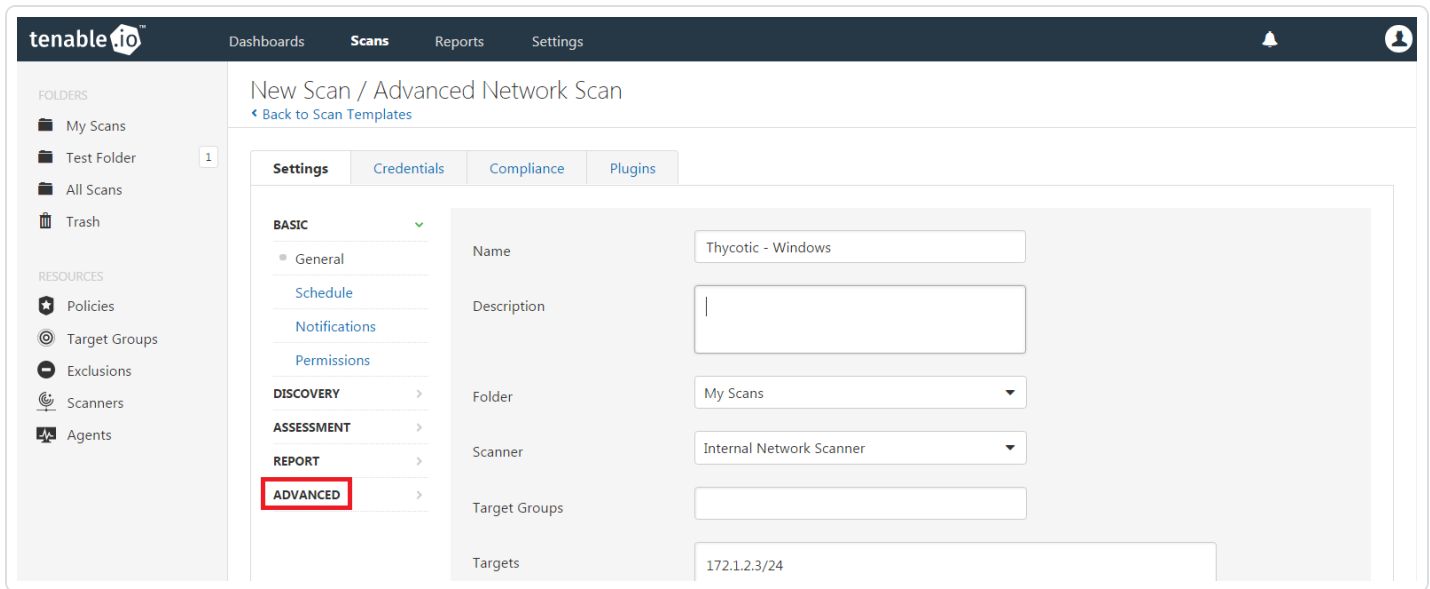
Once the scan has completed, select the completed scan and look for “Plugin ID 12634”, which validates that authentication was successful. If the authentication is not successful, refer to the “Troubleshooting” section of this document.



# Troubleshooting

Tenable Vulnerability Management offers the ability to enable plugin debugging, which will allow for easier troubleshooting and resolution should issues arise. Enabling plugin debugging attaches available debug logs from plugins to the vulnerability output of the scan it is enabled on.

To enable plugin debugging, navigate to scan **Settings** and click **Advanced** in the left-hand menu.



Select the **Enable plugin debugging** checkbox and click **Save** to finalize the change.

